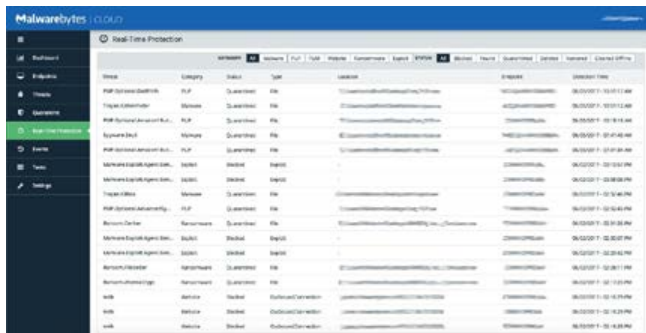# Malwarebytes

Malwarebytes Endpoint Protection

Advanced threat prevention

The most effective protection strategy starts with proactive prevention, but the best prevention approach won't be found with a silver bullet. In fact, security experts advise against relying solely on a single technology or technique to protect business endpoints. Effective prevention requires a layered approach capable of addressing not only today's threats, but preventing tomorrow's as well.

Malwarebytes Endpoint Protection is an advanced threat prevention solution for endpoints that uses a layered approach with multiple detection techniques. This provides businesses with full attack chain protection against both known and unknown malware, ransomware, and zero-hour threats. Unified onto a single agent, Malwarebytes Endpoint Protection reduces the complexity and costs often associated with deploying multiple individual solutions.

The industry's best-informed telemetry drives the efficacy of Malwarebytes Endpoint Protection detection techniques. Malwarebytes is the gold standard for providing complete and thorough remediation of threats when existing security solutions fail, evidenced by 500,000 consumers and businesses downloading Malwarebytes technology daily. Malwarebytes finds and remediates 3 million infections every day. This unique telemetry provides insight into the threats and techniques that are succeeding in the wild and offers a better understanding of what makes these attacks effective and how to best counter them.

Malwarebytes cloud console Real-Time Protection Key benefits

TECHNICAL FEATURES

ENDPOINT PROTECTION

Web Protection
Prevents access to malicious websites, ad networks, scammer networks, and bad neighborhoods

Application Hardening
Reduces vulnerability exploit surface and proactively detects fingerprinting attempts used by advanced attacks

Exploit Mitigation
Proactively detects and blocks attempts to abuse vulnerabilities and remotely execute code on the endpoint

Application Behavior Protection
Prevents applications from being leveraged to infect the endpoint

Anomaly Detection
Proactively identifies viruses and malware through machine learning techniques

Payload Analysis
Identifies entire families of known and relevant malware with heuristic and behavioral rules

Ransomware Mitigation
Detects and blocks ransomware via behavioral monitoring technology

Key Benefits

Layered detection techniques

Malwarebytes Endpoint Protection employs multiple techniques to identify and defend against attacks at all stages of the attack chain using a highly effective mix of signature-less and matching-technology layers working both pre- and post-execution. Leveraging the best-informed telemetry, the pre-execution techniques are updated to continually drive toward earlier detection in the infection chain. Malwarebytes Endpoint Protection offers Real Time Protection for both Windows and Mac.

Complete and thorough remediation

Malwarebytes Endpoint Protection leverages our Linking Engine technology to remove all traces of infections and related artifacts—not just the primary threat payload. This signature-less approach speeds up threat scans and saves time normally spent wiping and re-imaging endpoints.

Cloud-enabled management

Malwarebytes Endpoint Protection is delivered via our Malwarebytes cloud-based endpoint management platform. This cloud platform reduces complexity, making it easy to deploy and manage Malwarebytes Endpoint Protection and other Malwarebytes solutions, regardless of the number of endpoints. This centralized cloud-console eliminates the need to acquire and maintain on-premises hardware.

REQUEST A TRIAL

Visit
malwarebytes.com/business/trial/

SYSTEM REQUIREMENTS

Included Components
Malwarebytes cloud platform
Malwarebytes Endpoint Protection
(persistent Windows agent)
Email and phone support

Hardware Requirements
Windows
CPU: 1 GHz
RAM: 1 GB (clients); 2 GB (servers)Disk space: 100 MB (program + logs)
Active Internet connection
Mac
Any Apple device that supports Mac OS X (10.10 or newer)
Active Internet connection

Supported Operating Systems
Windows 10® (32-bit, 64-bit)
Windows 8.1® (32-bit, 64-bit)
Windows 8® (32-bit, 64-bit)
Windows 7® (32-bit, 64-bit)
Windows Vista® (32-bit, 64-bit)
Windows XP® with SP3 (32-bit only)
Windows Server 2016® (32-bit, 64-bit)
Windows Server 2012/2012R2® (32-bit, 64-bit)
Windows Small Business Server 2011
Windows Server 2008/2008R2® (32-bit, 64-bit)
Windows Server 2003® (32-bit only)
macOS 10.13 (High Sierra)
macOS 10.12 (Sierra)
macOS 10.11 (El Capitan)
macOS 10.10 (Yosemite)

Please note that Windows servers using the Server Core installation process are specifically excluded.

Windows Action Center integration not supported for Windows Server operating systems.

malwarebytes.com/business   corporate-sales@malwarebytes.com   1.800.520.2796

Malwarebytes is a cybersecurity company that millions worldwide trust. Malwarebytes proactively protects people and businesses against malicious threats, including ransomware, that traditional antivirus solutions miss. The company's flagship product uses signature-less technologies to detect and stop a cyberattack before damage occurs. Learn more at www.malwarebytes.com.